Using ISO/IEC 24727 for mobile devices

Jan Eichholz[1] · Detlef Hühnlein[2] · Manuel Bach[3]

[1]Giesecke & Devrient GmbH, jan.eichholz@gi-de.com
[2]secunet Security Networks AG, detlef.huehnlein@secunet.com
[3]Bundesamt für Sicherheit in der Informationstechnik, manuel.bach@bsi.bund.de

Abstract: The forthcoming ISO/IEC 24727 series of standards **[ISO24727]** defines architectures and application programming interfaces for electronic identity cards (eID). As there are already many initiatives around the globe (e.g. in the USA, Australia and Europe) which are about to use this standard in major eID-projects, it may be expected, that this standard will provide a major contribution for global eID interoperability and will become widely adopted in near future. On the other hand there is an ever increasing trend for mobility and the ubiquitous use of portable devices as well as first national eID-projects, which support mobile devices. Therefore it is natural to investigate how ISO/IEC 24727 may be used with mobile devices. The present contribution provides a brief overview of this standard and discusses different options for using this standard in a mobile environment.

1 Introduction

Against the background of the US Government Smart Card Interoperability Specification **[NIST-GSCIS]** and the activities around the Personal Identity Verification (PIV) program **[NIST-PIV]** the National Institute of Standards and Technology (NIST) initiated the development of the ISO/IEC 24727 series of standards (cf. **[ISO24727]**, **[NIST-SMP]**) which defines architectures and application programming interfaces for electronic identity cards (eID). This standard will also be adopted by the Australian Government (cf. **[AGIMO-AGSF]**) and it forms the basis of the European Citizen Card Application Interface specification **[CEN15480]** and the German eCard-API-Framework **[BSI-TR03112]**. Therefore it may be expected, that ISO/IEC 24727 will play a major role in global eID interoperability and will become widely adopted in near future.

On the other hand there is an ever increasing trend for mobility and the ubiquitous use of portable devices (cf. **[WCIS]**, **[MC07]**) and first national eID-projects are supporting portable devices (cf. **[A-SIT-ACC]**, **[B-WPKI-F]**). Therefore it is natural to investigate how ISO/IEC 24727 may be used with mobile devices.

The present contribution provides in Section 2 a brief overview of the ISO/IEC 24727 architecture and discusses in Section 3 different options for using this standard in a mobile environment. Section 4 summarizes the main aspects of the present contribution and draws conclusions.

2 ISO/IEC 24727 in a nutshell

The architecture defined in Part 1 of **[ISO24727]** assumes that a Client Application uses the functionality of cryptographic tokens using the *Service Access Interface* defined in Part 3 of the standard series.

This interface comprises generic functions which allow to establish (cryptographically protected) connections to card-applications, manage those card-applications, store and retrieve data, perform cryptographic operations, manage the related key material (so called Differential-Identities (DID)) and manage access rights for data, keys and services provided by card-applications.

The Service Access Layer (SAL) maps the generic requests at the Service Access Interface to APDUs of the *Generic Card Interface* defined in Part 2, which allows a subset of the commands and options defined in **[ISO7816]** (Part 4, 8 and 9). If the cryptographic token does not support those standard-commands directly they may be translated by the Generic Card Layer before they are sent to the Interface Device (IFD) Layer using the `Transmit`-command, which is – as other IFD-related commands in the IFD-API – defined in Part 4 of **[ISO24727]**.

Furthermore there is a "dispatcher", which redirects Web Service requests to remote software stacks and establishes trusted channels e.g. using **[RFC4346]**, if required.

The ISO/IEC 24727 architecture is extensible in two ways. First it allows the execution of arbitrary card-application services using the SAL-functions `ExecuteAction` and `CardApplicationServiceDescribe`. Second it supports arbitrary cryptographic (authentication) protocols because all DID-related functions have generic parameters, which are of an "open type", which is protocol dependent. We will return to the second alternative in Section 3.2 when we sketch such a "protocol" tailored for mobile devices.

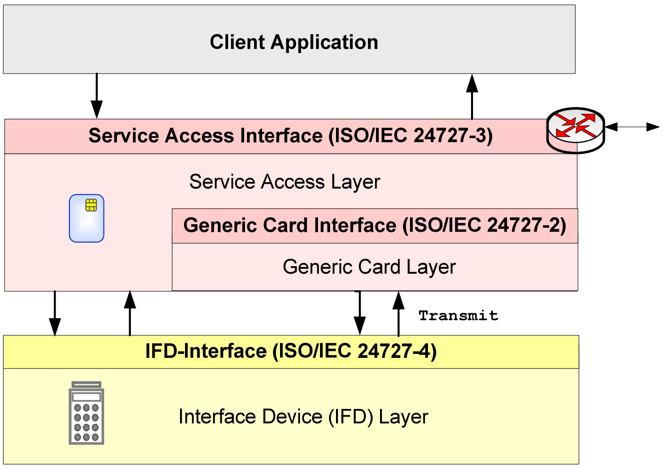
Client Application
Service Access Interface (ISO/IEC 24727-3)
Service Access Layer
Generic Card Interface (ISO/IEC 24727-2)
Generic Card Layer
Transmit
IFD-Interface (ISO/IEC 24727-4)
Interface Device (IFD) Layer

Figure 1: ISO/IEC 24727 Architecture

3 Using ISO/IEC 24727 with mobile devices

Depending on the use case and the capabilities of the mobile device there are various possible integration scenarios. Among those we will focus on two cases, which seem to cover a large proportion of currently available mobile devices:

- Cell phones with support for Java^{TM} Mobile Edition (JME) (see Section 3.1) and
- other devices within a Mobile Signature Services (MSS) based architecture (see Section 3.2).

3.1 Java^{TM} Micro Edition based solution

The Java^{TM} Micro Edition (JME) is the dominating open platform for cell phones. Since everything has started in the year 2000 with the definition of the Mobile Information Device Profile (MIDP) **[JSR271]** the platform has grown over the years and is nowadays covering a wide variety of functionality. The basic stack is defined within the Mobile Service Architecture (MSA) **[JSR248]** and the Connected Limited Device Configuration (CLDC) **[JSR139]**. Additionally, a couple of additional Java Specification Requests (JSR's) are adding specific functionality to the basic platform. In the context of eID, the following JSR's are especially important:

- JSR 177 (Security and Trust Service, **[JSR177]**) is defining the interface to an embedded security element (e.g. SIM),
- JSR 257 (Contactless Communication API, **[JSR257]**) defines the interfaces for contactless communication (RFID, NFC) and
- JSR 279 (Service Connection API for Java^{TM} ME, **[JSR279]**) offers the functionality to use and offer web services on a mobile device.

Figure 2 shows the interaction of the different software components with the security element (e.g. SIM card), the eService and an eID token.

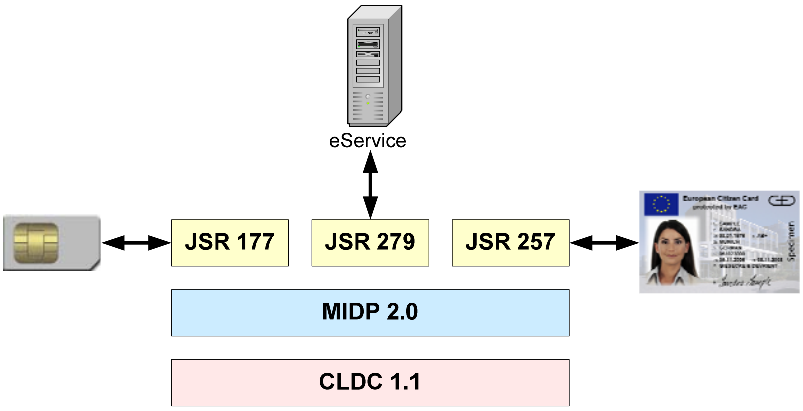

Figure 2: Java^{TM} Micro Edition based Architecture

In an ISO/IEC 24727 environment, the eService will use the standardized web service interfaces to communicate with the mobile device. To support complex protocols, like the General Authentication Procedure defined in **[BSI-TR3110]**, the mobile device should offer the Service Access Interface and the IFD-Interface as web service. In the future, the goal should be to offer a JSR, which is adding the ISO/IEC 24727 interfaces to the JME platform.

In the meantime, a client application on the device (MIDlet), which is based on the above listed JSR's, can add the necessary web services by its own (see Figure 3).

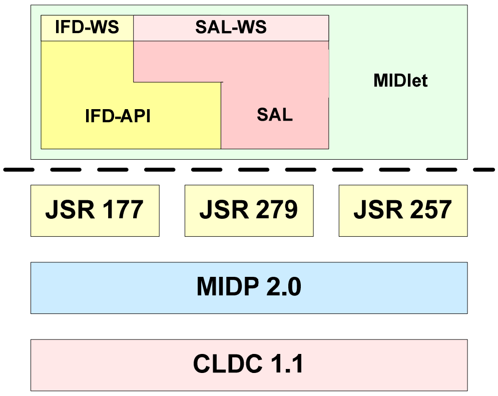

Figure 3: MIDlet based ISO/IEC 24727 Implementation

3.2 Mobile Signature Service based solution

In this case the integration will not take place within the mobile device but rather in the Service Access Layer (SAL) of the Application Provider (AP). This SAL has a "virtual card-application" embedded, which allows to communicate with a Mobile Signature Service Provider (MSSP) using the messages defined in **[ETSI-102204]**. For this purpose there will be an MSS-specific ISO/IEC 24727-protocol, in which the (keys of the) mobile users are represented as Differential-Identities.

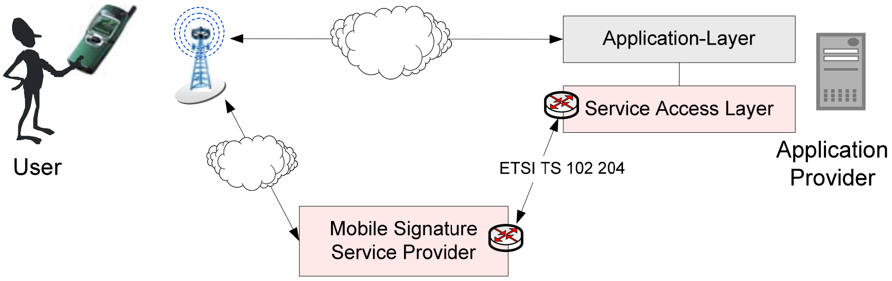

Figure 4: System architecture for MSS-based solution

We will briefly sketch how the main functions of **[ISO24727]** Part 3 map to functions defined in **[ETSI-102204]**[1]:

[ISO24727] Part 3	[ETSI-102204]	Note
CardApplication Path	/	Besides path-information of regular card-applications, CardApplication Path will also return a path to the „virtual card-application“ for **[ETSI-102204]**.
CardApplication StartSession	MSS_HandshakeReq	Using this function the AP and the MSSP agree on security mechanisms for further requests and responses.
DIDCreate / DIDUpdate	MSS_RegistrationReq	The keys of the mobile users are represented as Differential-Identites (DID). Consequently the creation of a DID corresponds to the registration of a user.
DIDGet	MSS_ProfileReq / MSS_StatusReq	DIDGet will be used to obtain information about a user profile and the status of a current transaction.
DIDAuthenticate	MSS_SignatureReq	Using the signing capability of the mobile device it is possible to design a challenge-response protocol for authentication.
Sign	MSS_SignatureReq	The signing capability of the mobile device may be also be used via the Sign function. As in **[BSI-TR03112]** the low level Sign function may be wrapped by a SignatureRequest according to **[OASIS-DSS]**.

Table 1: Mapping ISO/IEC 24727-3 to ETSI TS 102 204

4 Conclusion

In the current paper we briefly recalled the ISO/IEC 24727 architecture **[ISO24727]** and sketched two possibilities how this software stack may be used with mobile devices, which either support the Java™ Mobile Edition (JME) platform (see Section 3.1) or the Mobile Signature Services interfaces (see Section 3.2). While the ISO/IEC 24727 interfaces can be easily supported in both cases, the JME-based variant seems to be especially interesting for future developments, as it does not require a special provider infrastructure and may support a broader variety of NFC-related use cases in the future.

[1] Note that a similar mapping could be defined for other existing architectures and interfaces, as used for the Austrian Citizen Card **[A-SIT-ACC]** for example.

5 References

[AGIMO-AGSF] Australian Government Information Management Office (AGIMO): *Australian Government Smartcard Framework*, Phase 2 – Version 0.12, Standards and Model Specification – Part c, March 2007, http://www.agimo.gov.au/__data/assets/pdf_file/0008/56249/Standards_and_Model_Specification_-_Part_c_-_Version_0.12.pdf

[A-SIT-ACC] A-SIT: *The Austrian Citizen Card*, Overview of Version 1.2.0, May 14th 2004, http://www.buergerkarte.at/konzept/securitylayer/spezifikation/20040514/Index.en.html

[BSI-TR3110] BSI: *Advanced Security Mechanism for Machine Readable Travel Documents – Extended Access Control (EAC)*, Technical Directive of the Federal Office for Information Security Nr. 03110, BSI TR-03110, Version 2.0 – Public Beta 3, 2007

[BSI-TR03112] BSI: *eCard-API-Framework*, Technical Directive of the Federal Office for Information Security Nr. 03112, BSI TR-03112, Version 0.9, 2007

[B-WPKI-F] Baltic WPKI Forum: *Wiki of the Baltic WPKI Forum*, http://wpki.eu

[CEN15480] CEN: *Identification card systems — European Citizen Card*, CEN TS 15480 (Part 1-4), 2007

[ETSI-102204] ETSI: *Mobile Signature Service - Web Service Interface*, Technical Specification TS 102 204 V1.1.4, via http://portal.etsi.org/docbox/EC_Files/EC_Files/ts_102204v010104p.pdf

[ISO7816] ISO/IEC: *Identification cards – Integrated circuit cards*, ISO/IEC 7816 (Part 1-13 & 15)

[ISO24727] ISO/IEC: *Identification cards – Integrated circuit cards programming interfaces*, ISO/IEC 24727 (Part 1-5)

[JSR139] JCP: *Connected Limited Device Configuration 1.1*, Java Specification Request (JSR) 139, http://www.jcp.org/en/jsr/detail?id=139

[JSR177] JCP: *Security and Trust Services API for J2ME™*, Java Specification Request (JSR) 177, http://www.jcp.org/en/jsr/detail?id=177

[JSR248] JCP: *Mobile Service Architecture*, Java Specification Request (JSR) 248, http://www.jcp.org/en/jsr/detail?id=248

[JSR257] JCP: *Contactless Communication API*, Java Specification Request (JSR) 257 http://www.jcp.org/en/jsr/detail?id=257

[JSR271] JCP: *Mobile Information Device Profile 3*, Java Specification Request (JSR) 271, http://www.jcp.org/en/jsr/detail?id=271

[JSR279] JCP: *Service Connection API for Java™ ME*, Java Specification Request (JSR) 279, http://www.jcp.org/en/jsr/detail?id=279

[MC07] Mobileconnect: *Study: Mobile data revenues will increase to more than 200 Billion $US in 2011*, in German, http://www.mobileconnect.ch/de/2007/03/05/studie-mobile-datenumsatze-steigen-auf-uber-200-milliarden-us-in-2011/

[NIST-GSCIS] NIST: *Government Smart Card Interoperability Specification*, Version 2.1., July 2003, http://csrc.nist.gov/publications/nistir/nistir-6887.pdf

[NIST-PIV] NIST: *Personal Identity Verification (PIV) of Federal Employees and Contractors*, FIPS PUB 201-1, March 2006, http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

[NIST-SMP] NIST: *Standard and Metrics Project*, http://www.itl.nist.gov/ITLPrograms/IDMS/external/standards_metrics.html

[OASIS-DSS] OASIS: *Digital Signature Service Core Protocols, Elements, and Bindings*, Version 1.0, OASIS Standard, via http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.pdf

[RFC4346]	E. Rescorla, T. Dierks: *The Transport Layer Security (TLS) Protocol – Version 1.1*, RFC 4346, April 2006, http://www.ietf.org/rfc/rfc4346.txt
[WCIS]	Informa Telecoms & Media: *World Cellular Information Service*, http://www.wcisdata.com/